United States and the United Kingdom Sanction Members of Russian State Intelligence-Sponsored Advanced Persistent Threat Group

December 7, 2023

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC), in coordination with the United Kingdom, designated two individuals associated with an advanced persistent threat (APT) group that is sponsored by the Russian Federal Security Service (FSB) and has targeted individuals and entities in the United States, United Kingdom, and other allied and partner countries.

"As we have stressed through our bilateral actions over the past year, the United States and the United Kingdom stand together, steadfast against the Kremlin and its state-sponsored malicious cyber groups' efforts to target our democracies," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "We will continue to leverage our collective tools and authorities to protect our citizens, our government networks, and our democratic processes."

The United Kingdom has sanctioned two individuals for engaging in spear phishing operations with the intention to use information obtained to undermine UK democratic processes. The United States, in support of and in solidarity with the United Kingdom, has also taken action against the same individuals, identifying their connection to the FSB unit and its activity that has targeted U.S. critical government networks.

FSB-SPONSORED SPEAR PHISHING

The Kremlin uses the FSB, one of its intelligence and law enforcement agencies, to advance the Kremlin's interests and to try to undermine the interests of the United States and its allies and partners. The FSB employs its cyber capabilities to refine its espionage, influence, and intrusion campaigns.

A unit within the FSB is responsible for an APT that has targeted the United States and other nations. The FSB unit, characterized by its highly tailored spear phishing, has been given several monikers by private cybersecurity firms, which includes "Callisto" or "Callisto Group,"

"Seaborgium," "Coldriver," "Star Blizzard," "Gossamer Bear," "ReUse Team," "Dancing Salome," and "BlueCharlie," among others.

Since as early as 2016, FSB-sponsored spear phishing campaigns have focused their targeting on the webmail accounts of entities associated with government, military, private organizations and news media across the globe and has expanded to include accounts of U.S., UK, and North Atlantic Treaty Organization (NATO) countries' government, military, and government affiliates.

The FSB's spear phishing campaigns have been designed to gain access to targeted email accounts, to maintain persistent access to the accounts and associated networks, and to obtain and potentially exfiltrate sensitive information to advance the Kremlin's policy goals. For example, they have been linked to hack-and-leak operations, where stolen and leaked information is used to shape narratives in targeted countries and have conducted highly tailored spear phishing campaigns aimed at harvesting webmail, corporate, and governmental credentials.

In 2022, FSB actors were responsible for malicious cyber activity directed at facilities of a U.S. government agency. The malicious activity included impersonating agency employees and one Department of State employee by creating spoofed email accounts for the purpose of mimicking these employees in order to send spear phishing emails to unsuspecting and specifically targeted employees at the facilities.

FSB SPEAR PHISHING ACTORS

Two individuals associated with these spear phishing activities are **Ruslan Aleksandrovich Peretyatko** (**Peretyatko**), an FSB officer, and **Andrey Stanislavovich Korinets** (**Korinets**), an IT worker in Syktyvkar, Russia.

Between at least 2016 and 2020, **Korinets** fraudulently created and registered malicious domain infrastructure for FSB spear phishing campaigns. He would anonymously create shortened URL links that would be embedded in spear phishing emails. **Korinets** created at least 39 domains through 5 different domain registrars, using aliases and fake addresses in an attempt to obfuscate himself from the domains. Since the date of its activation until late 2019, a spoofed email account intended to mimic a retired U.S. Air Force general had sent at least 20 spear phishing emails, which included domains created by **Korinets**.

Also between at least 2016 and 2020, **Peretyatko** has used several email addresses that were designed to mimic legitimate management accounts of well-known technology companies to send spear phishing emails, some of which contained the domain infrastructure created by **Korinets**. In 2017, **Peretyatko** used a fraudulent email account to send spear phishing emails purporting to be from a major software company that directed victims to change their account password in an attempt to harvest their credentials; the link re-directed to a malicious domain created by **Korinets**.

Peretyatko and other FSB officers responsible for the spear phishing campaigns have researched new tools that would support their malicious cyber activities. One of the tools included malware that allows for the evasion of two factor authentication, another permits for the control of a device with limited risk of detection, and a third that allows access to webmail inboxes.

Korinets and **Peretyatko** are being designated pursuant to E.O. 13694, as amended by E.O. 13757, for being responsible for or complicit in, or having engaged in, directly or indirectly, a cyber-enabled activity identified pursuant to E.O. 13694, as amended.

In addition to the United Kingdom's action and OFAC's designation, the U.S. Attorney's Office of the Department of Justice's Northern District of California has unsealed indictments of **Korinets** and **Peretyatko** for their roles in a criminal hacking conspiracy that included the targeting of U.S.-based entities and individuals, including employees of U.S. Department of Energy facilities. Similar to the United Kingdom's actions imposing sanctions, the Department of Justice's charges also allege the activity was conducted by a unit subordinate to the FSB.

Concurrently, the U.S. Department of State's Rewards for Justice (RFJ) program is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Under this reward offer, the RFJ program is seeking information leading to the location or identification of **Peretyatko** and **Korinets**.

Additionally, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has published an advisory and an alert related to the malicious cyber activities with which **Peretyatko** and **Korinets** are associated.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the individuals described above that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC's regulations generally prohibit all dealings by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of a blocked or designated person.

In addition, persons that engage in certain transactions with the individuals designated today may themselves be exposed to sanctions.

The power and integrity of sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897 here. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

Click here for more information on the individuals and entities designated today.

For information on spear phishing, please visit CISA's General Security Postcard on Phishing .

To report a cyber-crime, contact the Federal Bureau of Investigation's Internet Crime Complaint Center.

###